INVICTUS
Education Trust

INFORMATION ASSET MANAGEMENT POLICY

Approved by Board of Directors
2 July 2018

To be reviewed by Board of Directors
July 2021

1. INTRODUCTION

Asset Management is the process of identifying; classifying, managing, recording and coordinating the Trust's assets (*physical, IT and information*) to ensure their security and the continued protection of any confidential data the Trust stores or gives people access to.

For the purposes of this policy and associated asset management processes, Invictus Education Trust defines an ***'Asset'*** as any item, system, application or entity that has potential or actual value to our organisation. Such assets include, but are not limited to:

- Information (*including personal data*)
    - Paper records
    - Electronic records
    - Files and folders
    - Software licenses
- Systems
- Computers or Workstations
- Networks
- Servers
- Hardware
- Software
- Telephony Systems
- Equipment
- Databases
- Technology
- Printers/Scanners
- Fax Machines

Assets can be both tangible and intangible and are of value to a business based on their importance, function and use. Whilst information is one of the Trust's most valuable assets, we understand the association and importance of the IT and physical assets that use, process, store and provide access to such information. As such, all forms of assets recorded by the Trust are valued and afforded a high level of protection and governance.

1.1. Definition

For the purposes of our Information Security program and the references in this policy, when we refer to '***Information Assets'*** we are collectively describing all assets within the Trust that are identified, recorded and secured. Most of our assets, including IT and physical are in place with the main purpose of holding and protecting personal information, and as such, we refer to all assets collectively as ***'Information Assets'***.

2. Policy Statement

The Trust understands the importance of identifying, recording and classifying our assets and utilise an Information Asset Register (IAR) to retain a complete list of all current assets, their location, value, access and other vital data. We have a responsibility to manage our physical and information assets, stemming from various legal, regulatory, contractual and business obligations: -

- General Data Protection Regulation (GDPR)
- Data Protection Bill
- Contractual (*client agreements, business objectives etc*)
- Security Requirements (*e.g. encryption, backups, updates etc*)
- Equipment Management (*service, replacement, disposal*)

The Trust ensures that all assets used and retained during business, are properly documented, are assigned an owner and are subject this policy and subsequent procedures. Managing our assets is paramount to the continuity of our core business – education and to the Trust's reputation. Assets are protected where applicable, further aiding in the protection of personal information and confidential data.

3. PURPOSE

The purpose of this policy is to achieve and maintain appropriate protection of organisational assets (*tangible and intangible*) and to document those assets to ensure knowledge and understanding of their value, purpose, risk and location. The Trust ensures that all assets are assigned an Information Asset Owner (IAO) who has overall responsibility for managing, updating, recording and destroying the asset.

The nature and value of every asset is documented and understood better enabling the Trust to restrict access where applicable, develop effective recovery and continuity programs and protect the interests and assets belonging to customers and clients.

Understanding the Trust's assets enables us to manage our organisation's information and systems and the risks associated with them. For this purpose, we utilise an Information Asset Register (IAR) to identify, document and map all information assets, and assign them an owner.

4. SCOPE

This policy applies to all staff within the Trust *(meaning permanent, fixed term, and temporary staff, any third-party representatives or sub-contractors, agency workers, volunteers, interns and agents engaged with the Trust in the UK),* and pertains to the processing of personal information. Adherence to this policy is mandatory and non-compliance could lead to disciplinary action.

5. OBJECTIVES

The Trust is committed to ensuring compliance with the rules, standards and regulations concerning asset management and the protection of the personal information in our remit. In education, we retain and process large volumes of personal data and therefore have strict aims and objectives for achieving and maintaining the appropriate protection of all organisational assets.

The Trust's objectives regarding asset management are to:

- Develop and maintain a defined and robust Asset Management Policy, including procedures for areas such as: -
    - Inventory of Information Assets
    - Assigning Asset Owners (Information Allocated Owner)
    - Information Classification
    - Personal Information
    - Confidential Information
    - Non-Disclosure Agreements
    - Information Sharing Measures

- Ensure that compliance all information assets have been identified
- Document all assets on the Information Asset Register (IAR) and assign each one an owner for monitoring and accountability
- Define the access to each asset and apply restrictions where applicable

- Maintain an up-to-date Records Management & Retention Policy
- Ensure that all staff are aware of the regulations and their obligations regarding asset management and to provide sufficient and adequate support and training in this regard

6. Guidelines and Procedures

The Trust takes several measures and steps to ensure that asset management is effective and adequate for managing and protection information. This policy is disseminated to all staff, who are aware of the value and importance of good records when it comes to the information held and processed by us.

6.1 Register of Information Assets

The Trust utilises an Information Asset Register (IAR) to document and categorise the assets under its remit. This not only enables the Trust to map the flow of data, but also serves as a tool for risk assessment and applying mitigating actions from the start.

The register contains all information, hardware, software, systems, applications and physical assets and is reviewed on a yearly basis, to ensure that the information is current and adequate. The register allows for descriptions and additional information fields, ensuring that all assets can be understood and assessed, but as a minimum standard, records:

- Asset ID
- Asset Type
- Description
- Information Asset Owner (IAO)
- Associated Risks
- Classification
- Location
- Format
- Retention Period
- Whether it contains personal data

6.2 Assigning Asset Owners

Each asset is assigned an owner (IAO) who is responsible for monitoring, maintaining and managing the asset and its use. This enables us to account for each asset and ensures that all risks have been identified and mitigated. The IAO is noted on the IAR and only they are permitted to effect change, on or with, the asset.

6.3 Unclassified & Short-Term Information Assets

Due to the volume of information used by the Trust, there are some assets, which are considered minor and as such are not subject to being classified or documented. This is only applicable where the asset has no security value and will not result in any internal or external risk if accessed. Such assets are also not assigned an owner or inventoried due to their limited nature.

The Trust operates under the GDPR and as such complies with the principle to never retain any information where there is no longer a purpose or reason to do so; however some records and information assets must be retained by law for specific retention periods and may come under our non-classification policy.

There is also a requirement due to the nature of education and our business needs to obtain some information assets for limited and short-term periods. Such assets can include letters, spreadsheets, temporary files and reports that are not classified or inventoried. All staff are aware of their responsibility for the documents they create, and this is further highlighted in the Trust's Data Retention Policy**.**

6.4 Remote Access & Bring Your Own Device (BYOD)

The Trust employees occasionally have a requirement to either use Trust assets (*physical and information*) outside of the office. Such instance can include during school trips, meetings, client visits and during travel. There are also facilities for using a self-owned device in the workplace, such as mobile phones and laptop. We understand the important of asset management for non-company devices and company assets used away from the office and have a robust ***Remote Access & BYOD Policy*** in place.

Regarding asset management when working remotely, it is the Trust's aim to protect our students, staff, other people (*clients, service providers, customers, suppliers etc*), organisational assets and systems when they are off-site. Our Information Security Program consists of several policies and procedures that overlap in this area and provide our robust and structured approach, controls and measures for protecting assets and access whilst off-site.

These documents include, but are not limited to

- Information Security Policy
- Risk Assessment Policy & Procedures
- Access Control & Password Policy
- Data Breach Policy
- Remote Access & BYOD Policy
- Asset Management Policy
- Information Asset Register (IAR)
- Clear Desk & Screen Policy
- Data Protection Policy & Procedure

6.5 Acceptable Use of Information Assets

Information assets are pivotal to the education of children and the core business of the Trust and to ensure a secure and effective environment, employees and third parties are provided with access and use of such assets to aid education of children and core business functions. The Trust's Acceptable Use Policy governs the use of information assets and failure to comply with these principles will result in disciplinary action and/or termination of contract.

The Trust has documented and implemented this acceptable use section in our Asset Management Policy to reiterate and provide guidelines on using our own and client assets. This information is disseminated to all employees, third parties and visitors to the Trust and forms part of our agreements and terms. All assets, with emphasis on client assets are used in a professional, lawful and ethical manner at all times and are audited on a regular basis to ensure adherence to this ethos.

Such acceptable use covers all assets and includes, but is not limited to:

- Email systems
- Internet usage
- Telephones (*including mobiles*)
- PDAs & laptops
- VPN Access, networks and portals

Specific emphasis is placed on adhering to this policy for employees who work from home and/or off-site and use or have access to information assets. Access and activities carried out during these times are logged and audited for compliance with the acceptable use ethos and standards.

Client assets and those with restricted access are not authorised for personal use under any circumstance. Assets are not available for personal use at any time and access to non-business-related internet is restricted. Employees are aware of the risks of using assets for personal use, such as personal emails that may contain viruses or permit access to restricted information.

6.5.1 Acceptable Use Standards

The Trust has documented and disseminated the below acceptable use standards to provide guidance and rules for using assets. These standards are adhered to by all employees and are a contractual part of any client visit or third party access to the Trust's information assets.

Employees, third parties and visitors are informed that they:

- Must not do anything to jeopardise the integrity of the systems, information assets or physical assets
- Are not permitted to use information assets for personal use
- Are not permitted to damage, change, reconfiguring or move any system or information asset with written authorisation and management supervision
- Are not permitted to remove any information asset from the Trust's buildings without written permission
- Must not attempt to access, delete, modify or disclose Information Assets belonging to other people without their permission
- Are not authorised to use any external systems, applications or technology with existing assets without permission and supervision
- Cannot disable or in any way alter system firewalls, anti-virus software or software/hardware protection applications
- Must not move any physical asset without written permission, including, but not limited to desktop PCs, printers, scanners, monitors or fax machines
- Are not permitted to load any unauthorised software onto the Trust's systems
- Must not connect to a the Trust's network or any equipment other than in approved circumstances
- Must not create, download, store or transmit unlawful or indecent material
- Are not authorised to purchase or otherwise acquire any technology assets without the knowledge and authorisation of the IT Network Managers
- Agree to abide by these rules at all times and confirm that the installation of any software on desktop PCs or laptops must only be carried out by IT
- Observe the Trust's Data Protection and Information Security policies and guidance in all instances

6.5.2 Internet & Email Usage

The internet is a pivotal part of the services offered by the Trust and as such, must be accessible to all students during the school day and to employees during their work hours. However, we recognise the security risks of using the internet and so access is only available through the Trust's local network or secured wireless network with the appropriate infrastructure and firewall protection. The internet is not permitted for personal use and certain sites are blocked by default to enforce this rule. The Trust have also restricted the sharing of files on certain systems and for some individuals, dependant on their need to use such facilities.

Email is necessary for the education and core business of the Trust and is afforded to all students and employees. This is our main communication tool and enables quick and effective access to other students, employees and clients. Email is accessible via secured connection and the sending of files or personal information is restricted to a User Required Level. Encryption methods are used and are detailed in our Encryption Policy, along with secure credentials.

6.6 Removable Media

The Trust defines *'removable media'* as any type of storage device or object that is physically able to be disconnected and removed from a system or computer whilst it is active. Such media types include, but are not limited to USB's, Media Cards, CDs, DVDs and SD cards.

We strictly control the use and oversight of removable media due to their nature and increased access and security risk. Removable media makes it easy for a person to move programs, data and content from one computer to another and as such, the Trust ensures that all employees and third parties abide by this policy and our removable media rules. Documented guidance for using removable media provides working practices for the Trust that can be adopted by all users, ensuring the safe storage, use and transfer of information.

We control the use of removable media devices, to enable us to:

- Ensure the access to information is limited and restricted dependant on its purpose and content
- Maintain the integrity of the data and protect its owner and/or source
- Prevent risks and/or security breaches through loss of assets
- Comply with regulations, laws and contractual obligations
- Provide a safe and effective workplace for employees and clients
- Maintain high standards of securing and restricting personal information.
- Prohibit the disclosure of information, both for best practice and as applicable to the data protection laws

6.6.1 Using Removable Media Devices

Unless provided to a student or employee directly by the Trust, we prohibit the use or possession of any removable media devices on-site. Removable media devices pose a serious risk to the information held by the Trust and where there is a need for using such devices; these will be owned, controlled and provided by the Trust directly.

Where a student requires a removable media device for use internally or externally, they must request this directly with their Tutor/Teacher.

Where an employee requires a removable media device for use internally or externally, they must request this directly with their line manager.

All requests should state:

- The removable media device required
- The purpose of the device
- Duration needed for
- How it will be secured and protected during use
- Where the device will be used
- What assets the device will be connected to

All removable media devices and any associated equipment and software are only available through the Trust’s IT Network Managers, who will place orders and take receipt of any such devices. Where removable media is used to store important, essential or personal information, this will be done so as a backup format and is never the sole location of such data. Removable devices can become corrupt or inaccessible and there must be alternate and secure backups of all information.

For removable media devices that are needed for use outside of the Trust's premises please see our Remote Working Policy for use and guidelines. Strict encryption software is used on removable media devices that partition the media and enable a secure, segregated data section that is only accessible via login credentials and authentication.

The Trust uses the latest virus and malware checking software on all assets to ensure that where removal media devices are being used, these are scanned are authorised prior to allowing access to any networks, systems or servers.

Whilst removable media are in transit, they are secured through internal credential authentication and external security measures. These include the use of additional encryptions during transit.

6.7 Information Classification

When the Trust's records information assets on our Information Asset Register (IAR), each asset is given a classification to help describe the use, purpose, content and risk level associated with it. The Trust specifies five main classification types:

1. **Unclassified** - assets not of value and/or retained for a limited period where classification is not required or necessary
2. **Public** - information that is freely obtained from the public and as such, is not classified as being personal or confidential
3. **Internal** - physical or information assets that are solely for internal use and do not process external information or permit external access
4. **Personal** - information or a system that processes information that belongs to an individual and is classed as personal under the data protection laws
5. **Confidential** - private information or systems that must be secured at the highest level and are afforded access restrictions and high user authentication

When each asset is obtained, it is added to the IAR and is assessed and classified by the owner according to its content. The classification is then used to decide what access restriction need to be applied and the level of protection afforded to the asset. The classification along with the asset type, content and description are then used to assess the risk level associated with the information and mitigating action can then be applied.

6.8 Non-Disclosure & Confidentiality Agreements

The Trust uses a robust and predefined non-disclosure agreement with all employees as part of their employment contract. We also use such agreements for visitors to the Trust premises, during audits and where contracts, business relationship or supplier connections are formed. The non-disclosure agreement template is altered on a case-by-case basis to ensure that information seen, disclosed or shared during any relationship with the Trust, is secure and protected.

As part of the education of students and the nature of our business, the Trust often shares personal and confidential information with other service providers and clients and as such, relies on clauses and stipulations in our confidentiality agreements. Alongside encryptions and secure transfers, the Trust always assess the risk of disclosing any information against the purpose and reason for doing so.

Where information must be shared for educational/business interests or legal reasons, non-disclosure agreements, are signed by third parties, prior to any information being disclosed and reviews are conducted to ensure that they have adequate safeguards in place for information transfers. Please see our *Data Protection*

Policy & Procedures & *International Data Transfer Procedures* for information on secure file sharing and transfers.

6.9 Information Labelling, Handling and Disposal

The Trust employs a labelling system that categorises the content of systems, files, applications and documents, without the necessity of disclosing the actual contents. This enables our employees to understand what content or information resides on a system or in a location, without accessing or seeing the personal content. Labelling allows us to document and control information, whilst still respecting access restriction.

6.9.1 Disposal of Assets

How we dispose of assets is of paramount importance due to the nature of education and our business needs. We handle large volumes or personal data and utilise systems that retain and process such data daily. Please refer to our Retention & Erasure Policy, which details how we dispose of all data, hardware, devices and records.

Reformatting of systems and hardware is our default position. However, great care is always exercised when disposing of any equipment, which has been used in the processing of information, as there is always a possibility that some information may remain.

7. RESPONSIBILITIES

The Trust will ensure that all staff are provided with the time; training and support to learn understand and implement the Asset Management Policy and that direct asset owners are trained and supported in their role. Asset Management at the Trust is a top-down approach and every employee understands the importance of the information and assets in our possession.

7.1 Information Asset Owners (IAO)

IAO's act as the nominated owner of specific assets within the Trust and are responsible for maintaining the correct information on the IAR and for documenting and understanding how the asset is used, access and of value to the Trust. Any process or function that affects an asset must first be authorised by the IAO.

7.1.1 Managers and Supervisors

Headteachers and Senior Management Teams are held responsible for ensuring that any employee who reports to them is aware of this policy and has been provided with adequate time and resources to understand its contents and meaning.

Any documented manual, handbook, policy or procedures that is related to asset management must be accessible to all employees and managers must be approachable and available should employees have questions regarding assets or their management. Line managers are also responsible for liaising with the IAO(s) to ensure that effective and adequate training is provided to new staff and existing staff on a rolling basis regarding assets, with emphasis on information assets.

8.0 Monitoring and Review

This Policy is reviewed every three years by Invictus Education Trust Board of Directors. We will monitor the application and outcomes of this policy to ensure it is working effectively.